Remarks

Claim 32 has been amended to correct a grammatical error. Claims 1-34 remain pending in the Application. No new matter has been added. Entry of the amendment is respectfully requested. Reconsideration is respectfully requested.

Declaration Pursuant to 37 C.F.R. § 1.132

Enclosed herewith is a third Declaration pursuant to 37 C.F.R. § 1.132 which further establishes that the pending claims are not obvious in view of the applied art and that the applied art is inoperative and non-enabling with respect to the subject matter of the pending claims. The Declaration is from a person with actual knowledge of the relevant art and the level of ordinary skill in the art at the time of the invention and subsequent filing of the application.

In addition, it is well settled that "weight ought to be given to a persuasively supported statement of one skilled in the art on what was not obvious to him." *In re Lindell*, 385 F.2d 453, 155 USPQ 521 (CCPA 1967). Applicants respectfully submit that the Declaration provides such a statement in addition to establishing that one of ordinary skill in the art at the time of the invention would consider the applied art as being **inoperative and non-enabling** with respect to the subject matter of the claims in the present application. Thus, the Declaration provides factual evidence which disproves the pending rejections.

Rejections Under 35 U.S.C. § 103(a)

Claims 1-34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Cromer, et al., U.S. Publication No. 2002/0166072 ("Cromer"). These rejections are respectfully traversed.

Claims 1, 14, 16-17, 19-20 and 22

Claims 1, 16 and 19 are independent claims directed to methods involving an automated banking machine. Claims 14, 17 and 20 are independent claims directed to articles bearing computer executable instructions reciting method steps corresponding to the steps recited in respective claims 1, 16 and 19. Claim 22 is an independent claim directed to an automated banking machine.

Each of these claims recites a BIOS of an automated banking machine that specifies a drive that (when detected) requires the manual input by a user of a BIOS boot password prior to booting from the drive. Also the BIOS of the automated banking machine specifies a drive that does not require the manual input by a user of a BIOS boot password prior to booting from the drive.

This arrangement enables the automated banking machine to boot from its default internal hard drive automatically without user intervention. However, when an authorized technician wishes to conduct maintenance on the machine, the technician may attach a bootable portable drive and/or bootable media, which will be booted only after the person inputs a password that matches a password stored in the BIOS. With this configuration, the automated banking machine is operative to be booted by any portable drive and/or media the technician may chooses to use, as long as the technician can manually input the proper boot password stored in the BIOS.

Nowhere does Cromer disclose or suggest an automated banking machine or any other machine with such features and capabilities. Further, even with respect to generic PCs, Cromer does not disclose or suggest these features. Rather in Cromer, a computer boots to a detected drive by verifying (when configured to do so) that a hash of data stored on the drive (e.g. a model and serial number) matches corresponding data stored in a BIOS (paragraph [0027]). Cromer does not disclose or suggest, (or have any apparent reason for) after detection of bootable media for a designated drive, requiring that a user manually input a BIOS boot password in order to boot from the drive.

Thus each of claims 1, 14, 16-17, and 19-20 recites subject matter not disclosed or suggested by Cromer. For example nowhere does Cromer disclose or suggest the following combination of features, relationships and steps recited in claims 1 and 14:

- **detecting with a computer of an automated banking machine for the presence of a bootable media in at least one alternative storage device drive of the automated banking machine**
- **wherein when the bootable media of the at least one alternative storage device drive is detected in step (a), the booting of the computer includes requiring at least once for a user to input a password, wherein when the inputted password corresponds to the BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to the boot record on the bootable media of the at least one alternative storage device drive**

Also, for example, nowhere does Cromer disclose or suggest the following combination of features, relationships and steps recited in claims 16 and 17:

- **detecting with a computer of an automated banking machine, the presence of a first bootable media in at least one first storage device drive of the automated banking machine**
- **requiring at least once for a user to input the BIOS boot password, wherein when an inputted password corresponds to a BIOS boot password stored in the BIOS of the computer, the computer is booted responsive to a first boot record on the first bootable media**

Also, for example, nowhere does Cromer disclose or suggest the following combination of features, relationships and steps recited in claims 19 and 20:

- **detecting with a computer of an automated banking machine that a bootable media is present in at least one alternative storage device drive of the automated banking machine**
- **prompting at least once for a user to input the BIOS boot password**
- **determining that an inputted password corresponds to the BIOS boot password stored in the BIOS of the computer**
- **booting software of the computer responsive to a first boot record on the bootable media of the at least one alternative storage device drive**

Also, for example, nowhere does Cromer disclose or suggest the following combination of features and relationships recited in claim 22:

- **An automated banking machine comprising a computer**

- **wherein when the computer detects a bootable media associated with the at least one first storage device drive, the computer is operative to require a user to input a BIOS boot password through the at least one input device prior to booting responsive to a boot record associated with the bootable media of the at least one first storage device drive**

The Action appears to allege that Figure 2 and paragraph [0026] of Cromer discloses requiring a user to input a password when an alternative storage device drive is detected. Applicants' respectfully disagree.

Figure 2 and paragraph [0026] of Cromer shows that Cromer may require a password for booting to a device. However, as shown in Figure 2, item 128, and paragraph [0027], this password is not a user inputted password, but rather is acquired by the computer interrogating the device for the serial and model number stored thereon. Thus Cromer clearly does not disclose or suggest all of the features, relationships, and steps recited in the claims. It follows that the Office has not established a case of *prima facie* obviousness.

In addition, it would not be obvious to one of ordinary skill in the art to modify Cromer in a manner that would correspond to the recited subject matter. In paragraph [0010], Cromer holds out as a problem with the prior art, that "it is a trivial exercise for an unauthorized user to connect his own hard disk drive in lieu of the password protected hard disk drive". Cromer's solution to making computers more secure and to prevent any portable unknown drive from being used to boot a computer, is to require the computer to be configured to only boot from devices that internally include data (e.g. model and serial number) that has been previously coupled to the BIOS of the computer. By calling out the disadvantage of using unknown hard disk drives (e.g.

in paragraphs [0010] and [0028]), Cromer teaches away from Applicants' invention (which enables a technician to boot from a new and unknown drive/media) by teaching a system that prevents an unknown device (not coupled to a BIOS) from being booted. Further, since Cromer has provided a method for securely booting from drives (via coupling the drive to the BIOS), there is no apparent reason for one of ordinary skill in the art at the time of the invention to further modify Cromer to require the input of a BIOS boot password, prior to booting from the drive.

In addition, Cromer does not disclose or suggest modifying an automated banking machine to include its described BIOS. An automated banking machine includes ports, such as USB ports inside a locked enclosure and/or a locked safe. Cromer does not provide any teaching or suggestion that such physical security is inadequate.

Further, paragraph [0007] of Cromer (referenced in the Action to support obviousness) describes the lack of security associated with an unattended conventional PC. However, automated banking machines are not conventional PCs. For example, even when automated banking machines are unattended, the physical security of ports inside a locked enclosure or chest makes them non-analogous to a vulnerable unattended PC. Thus Cromer does not provide any motivation to one of ordinary skill in the art at the time of the invention to modify an automated banking machine to use his described BIOS.

Cromer does not disclose or suggest each of the features, relationships, and steps recited in claims 1, 14, 16-17, 19-20, and 22 and the Office has not established *prima facie* obviousness. Also, because there is no apparent reason in the prior art or any other rationale for combining and/or modifying features of the applied art so as to produce Applicants' invention, it is respectfully submitted that claims 1, 14, 16-17, 19-20, and 22 are allowable for these reasons.

Therefore, it is respectfully submitted that the 35 U.S.C. § 103(a) rejection of these claims should be withdrawn. It follows that claims 1-13, 15, 18, 21, and 23-34 which depend from the independent claims are likewise allowable.

The Dependent Claims

Each of the dependent claims depends directly or indirectly from an independent claim. The independent claims have been previously shown to be allowable. Thus, it is asserted that the dependent claims are allowable on the same basis.

Furthermore, each of the dependent claims additionally recites specific features and relationships that patentably distinguish the claimed invention over the applied art. The applied art does not teach the features and relationships that are specifically recited in the dependent claims. Thus, it is respectfully submitted that the dependent claims are further allowable due to the recitation of such additional features and relationships.

Claims 2 and 23

With respect to claims 2 and 23, nowhere does Cromer disclose or suggest that when a bootable media of an alternative storage device drive is detected and a BIOS boot password is not inputted within a predetermined amount of time by a user, the computer is booted responsive to the boot record of the bootable media of the default storage device drive.

The Action asserts that Cromer shows this recited subject matter in Figure 2. Applicants respectfully disagree. Figure 2A of Cromer shows that if an interrogated device does not supply a correct password (e.g. is model and serial number), then another device is selected. Nowhere does Cromer disclose or suggest monitoring for an input of a password within a predetermined

amount of time. If Cromer's computer is unable to interrogate a device, or if Cromer's computer receives an incorrect model and serial number from a device, then Cromer simply selects another device. There is no need in Cromer to base selection of a default storage device drive on whether a predetermined amount of time has passed without receiving a manual input of a password.

The Action has not established a case of *prima facie* obviousness with respect to claims 2 and 23. Further, the Action has not provided any apparent reason or rationale to modify the applied art to correspond to the subject matter recited in claims 2 and 23.

Withdrawal of the rejections of claims 2 and 23 is respectfully requested.

Claims 4 and 34

With respect to claims 4 and 34, nowhere does Cromer disclose or suggest **a cash dispenser or dispensing cash from a cash dispenser**. Further, automated banking machines having cash dispensers are not analogous to Cromer's described vulnerable unattended conventional PC. As described previously with respect to claim 1, Cromer does not provide any teaching or suggestion that the physical security of an automated banking machine is inadequate, and thus does not provide any motivation to modify an automated banking machine that dispenses cash to include his described BIOS.

The Action has not established a case of *prima facie* obviousness with respect to claims 4 and 34. Further, the Action has not provided any apparent reason or rationale to modify the applied art to correspond to the subject matter recited in claims 4 and 34.

Withdrawal of the rejections of claims 4 and 34 is respectfully requested.

Claims 5 and 32

With respect to claims 5 and 32, nowhere does Cromer disclose or suggest receiving a first input that is representative of a request to run a BIOS setup program and prior to running the BIOS setup program, requiring a user to provide a second input that corresponds to the BIOS boot password stored in the BIOS (which is the same password required to be inputted by the user to boot from a detected bootable media).

For example, although Cromer indicates that a configuration password (item 108 in Figure 2A and paragraph [0022]) is needed to configure a BIOS, nowhere does Cromer disclose or suggest that this same configuration password is also required to be inputted by the user to boot from a detected boot media of an alterative storage device drive. Further, as discussed previously, Cromer's password for booting from a device corresponds to a hash of the model and serial number read from the device. It would not be obvious to one of ordinary skill in the art at the time of the invention to make Cromer's configuration password correspond to a model and serial number of a device. Further, this would pose a security risk to the computer (i.e. the configuration password could be stolen/hacked), because the model and serial number of a drive is readily viewable in the clear by a user accessing the properties of the drive.

The Action has not established a case of *prima facie* obviousness with respect to claims 5 and 32. Further, the Action has not provided any apparent reason or rationale to modify the applied art to correspond to the subject matter recited in claims 5 and 32.

Withdrawal of the rejections of claims 5 and 32 is respectfully requested.

Conclusion

In conclusion, it was not known nor would it have been obvious to a person having ordinary skill in the art having full view of the cited references, to have produced the claimed features, relationships, and steps. Applicants respectfully submit that this application is in condition for allowance. The undersigned is willing to discuss any aspect of the application at the Office's convenience.

Respectfully submitted,

Ralph E. Jocke Reg. No. 31,029
WALKER & JOCKE
231 South Broadway
Medina, Ohio 44256
(330) 721-0000